Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) ~~Apparatus~~ An apparatus arranged to accept digital data as an input~~,~~ and to process ~~said~~ the data according to one of either the Secure Hash Algorithm (SHA-1) or Message Digest (MD5) algorithm to produce a fixed length output word, ~~said~~ the apparatus ~~including~~comprising:

~~•~~ a plurality of rotational registers for storing data, one of said registers ~~being~~ arranged to receive the input data; and

~~•~~ data stores for ~~initialisation~~initialization of some of said plurality of registers according to whether the SHA-1 or MD5 algorithm is used, said data stores including fixed data relating to SHA-1 and MD5 operation; and

~~•~~ a plurality of dedicated combinatorial logic circuits arranged to perform logic operations on data stored in selected ones of said plurality of registers.

2. (Currently Amended) ~~Apparatus as claimed in~~ The apparatus of claim 1 wherein the register arranged to receive the input data is arranged to receive said input data serially.

3. (Currently Amended) ~~Apparatus as claimed in claim 1 or 2~~ The apparatus of claim 1 wherein the registers and combinatorial logic circuits are interconnected for communication via a pair of data busses.

4. (Currently Amended) ~~Apparatus as claimed in~~ The apparatus of claim 3 wherein the registers and combinatorial logic circuits are connected to write to a respective bus via respective tristate buffers.

5. (Currently Amended) ~~Apparatus as claimed in any one of the preceding claims~~ The apparatus of claim 1 wherein the apparatus includes a control circuit arranged to generate individually gated clock signals for each register.

6. (Currently Amended) ~~Apparatus as claimed in~~ The apparatus of claim 5 wherein said control circuit is further arranged to generate individual enabling signals to control the tristate buffers.

7. (Currently Amended) ~~Apparatus as claimed in any one of the preceding claims~~ The apparatus of claim 1 wherein the rotational registers are arranged to be multiplexed prior to connection to a tristate buffer.

8. (Currently Amended) ~~Apparatus as claimed in any one of the preceding claims~~ The apparatus of claim 1 wherein the combinatorial logic circuits include a copy circuit, a shift left circuit, a NOT circuit, an ADD circuit, an OR circuit, an AND circuit and an XOR circuit.

9. (Currently Amended) ~~Apparatus as claimed in any one of the preceding claims~~ The apparatus of claim 1 wherein the apparatus is implemented as an integrated circuit.

10. (Currently Amended) ~~Apparatus as claimed in any one of the preceding claims~~ The apparatus of claim 1 wherein the apparatus further includes circuitry arranged to perform digital signature creation or authentication.

11. (New) A circuit, comprising:

a plurality of data storage registers for storing data to be processed;

a plurality of shift registers for temporary data storage;

a plurality of logic circuits for performing operations on data; and

a control circuit configured to control the data storage registers, the shift registers, and the logic circuits to selectively perform MD5 and SHA-1 operations on data.

12. (New) The circuit of claim 11, further comprising a plurality of initialization storage registers adapted to store and output initialization data for the MD5 and SHA-1 operations.

13. (New) The circuit of claim 12, comprising a read bus and a write bus selectively coupleable to the plurality of data storage registers, the plurality of shift registers, and the plurality of logic circuits by the control circuit.

14. (New) The circuit of claim 11, further comprising a multiplexer to multiplex outputs of the plurality of shift registers to the read bus.

15. (New) A circuit, comprising:

means for storing data to be processed;

means for temporarily storing data to be processed;

means for performing combinatorial logic operations on data; and

means for controlling coupling of the data storage means, the temporary data storage means, and the means for performing combinatorial logic operations to read and write busses to selectively perform MD5 and SHA-1 operations on data.

16. (New) The circuit of claim 15, further comprising means for storing data to initialize the circuit to perform MD5 and SHA-1 operations in response to commands from the control means.

17. (New) The circuit of claim 15, further comprising means for multiplexing outputs from the temporary data storage registers to the read bus in response to commands from the control means.

18. (New) The circuit of claim 17 wherein the temporary data storage means is configured to receive a stream of data and the circuit further comprises an output on which is generated data of a fixed length.

19. (New) A dual hash algorithm circuit, comprising:

a first bank and a second bank of data storage registers;

a first bank and a second bank of circular shift registers, including at least one register to receive a data stream as input to the circuit;

a bank of initialization data registers;

a bank of temporary data registers;

a plurality of combinatorial logic circuits;

a read bus and a write bus;

a control system for selectively coupling and uncoupling the first bank and second bank of data storage registers, the first bank and second bank of circular shift registers, the bank of initialization data registers, the bank of temporary data registers,

and the plurality of combinatorial logic circuits to the read bus and the write bus to selectively perform MD5 and SHA-1 operations on the data and to output data of a fixed length in accordance with the selected MD5 and SHA-1 operations.

20. (New) The circuit of claim 19 wherein the control system comprises a control circuit and tristate buffers to couple and uncouple the first bank and second bank of data storage registers, the first bank and second bank of circular shift registers, the bank of initialization data registers, the bank of temporary data registers, and the plurality of combinatorial logic circuits to the read and write busses in response to the control circuit.

21. (New) The circuit of claim 19, further comprising a multiplexer configured to multiplex outputs from the first bank and second bank of circular shift registers to the read bus.